

Before the
FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of)	
)	
IP-Enabled Services)	WC Docket No. 04-36
)	

MOTION TO ACCEPT LATE-FILED COMMENTS

The UNITED STATES DEPARTMENT OF DEFENSE (DoD), hereby respectfully submits this Motion to Accept Late-Filed Comments on the Commission's Notice of Proposed Rule Making in the proceeding captioned above.

In this proceeding, the Commission was seeking comment on issues relating to services and applications making use of the Internet Protocol (IP), including, but not limited to, voice over IP services. The Commission asked for comment on ways in which the Commission might properly categorize IP-enabled services; whether the Commission has jurisdiction over such services, and, if so, whether that jurisdiction is exclusive; the appropriate statutory classification of the services falling into each category of IP-enabled service; and which regulations, if any, should apply to services falling into each category.

The lengthy proposed rules could significantly impact the mission objectives and policy responsibilities of several DoD components; development of the Department's comments required extensive coordination prior to filing.

The Department submits that the acceptance of its Comments will contribute meaningfully to the development of a complete record to guide the Commission's decision making in this proceeding. The Commission itself, recognizing the novelty and complexity of

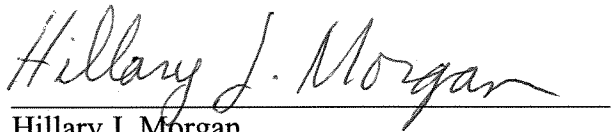
the issues raised in this proceeding, has also extended the period for reply comments (see *Wireline Competition Bureau Extends Reply Comment Deadlines For IP-Enabled Services Rulemaking And SBC's "IP Platform Services" Forbearance Petition*, DA 04-1685, June 9, 2004 [WC DOCKET NOS. 04-29, 04-36].)

Accordingly, for the foregoing reasons, DoD respectfully requests that the Commission grant this Motion and accept the attached Comments.

Respectfully submitted,

**UNITED STATES DEPARTMENT OF
DEFENSE**

By:

A handwritten signature in cursive script, reading "Hillary J. Morgan", written over a horizontal line.

Hillary J. Morgan
United States Department of Defense
Trial Attorney, Regulatory and International Law
Defense Information Systems Agency
701 S. Courthouse Road
Arlington, VA 22204
(703) 607-6092

Date: June 10, 2004

**BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554**

In the Matter of

FCC Review of Regulatory Requirements
for IP-Enabled Services

)
)
)
) WC Docket No. 04-36
)
)
)
)

TO: The Commission

**COMMENTS OF THE
DEPARTMENT OF DEFENSE**

TABLE OF CONTENTS

TABLE OF CONTENTS.....	ii
I. SUMMARY.....	1
II. STATEMENT OF INTEREST AND POSITION, NS/EP.....	3
IMPACT OF EMERGING IP-ENABLED SERVICES ON NS/EP.....	6
III. STATEMENT OF INTEREST AND POSITION, ASD/NII RESPONSIBILITIES.....	7
A. COMMUNICATIONS SECURITY MONITORING REQUIREMENTS.....	9
B. ENSURING APPROPRIATE USE, COMBATING MISUSE, DOD SYSTEMS...	10
1. 47 U.S.C. § 222, IP-ENABLED SERVICES & SERVICE PROVIDERS.....	11
2. INSPECTOR GENERAL AND LAW ENFORCEMENT REQUIREMENTS.....	13
C. NOTICE OF FOREIGN TRANSACTIONS.....	13
IV. CONCLUSION.....	15

Summary, Comments of the Department Of Defense

The Secretary of Defense, through duly authorized counsel, files these initial comments in this proposed rulemaking from two different perspectives. First, these comments address issues relating to the Department's role as a member of the National Communications System (NCS.) The second portion of this filing highlights concerns the DoD has with respect to possible impact on its own ongoing network security activities. The Commission is respectfully requested to consider adopting regulations based on the DoD equities raised in this filing, in order to support national security requirements in both the traditional telecommunications infrastructure and all elements of the information technology infrastructure subject to its jurisdiction.

In order to execute its assigned responsibilities in times of national emergency, domestic attack and crisis, robust, redundant, reliable communications are essential for the DoD. As the single largest user of national security emergency preparedness (NS/EP) priority services, the Department strongly supports the comments filed by the Department of Homeland Security on behalf of the NCS.

The Assistant Secretary of Defense for Networks and Information Integration, ASD(NII), is the Department's Chief Information Officer (CIO.) The Commission is invited to exercise some oversight over services employing Internet protocol applications and packet-switched technology, in order to serve the public interest. Ensuring appropriate technical means are provided by service providers, to enable access to DoD network data transmitted via IP-enabled services, would support the national defense, as would requiring foreign investors to provide pre-transaction notice before service affected by non-U.S. influence or control begins.

Washington, D.C. 20554

IP-Enabled Services

COMMENTS OF THE DEPARTMENT OF DEFENSE

¹ See 40 U.S.C. § 501(a)(2).

² E.g., IP-Enabled Services, WC Docket No. 04-36, Notice of Proposed Rulemaking, FCC 04-28 (Mar. 10, 2004) (IP Enabled Services) and Public Notice DA-04-888 (WC Docket No. 04-36) of March 29, 2004.

PART I

STATEMENT OF INTEREST AND POSTION: DOD'S ROLE AS A MEMBER OF THE NATIONAL COMMUNICATIONS SYSTEM (NCS), AND A USER OF NCS NATIONAL SERCURITY EMERGENCY PREPAREDNES PRIORITY SERVICES

By law, the National Communications System (NCS) functions of the Department of Defense (DoD) were among the federal activities transferred into the Department of Homeland Security (DHS.)³ The NCS itself consists of the telecommunications assets of the 23 major Federal Departments and Agencies represented on the NCS Committee of Principals (COP); DoD is one of the 23 elements that make up the NCS COP.⁴ The Secretary of Homeland Security is assigned the additional duty of Executive Agent of the NCS under the authority of Executive Order (EO) Number 12472,⁵ as amended by EO 13286.⁶ The Homeland Security Act of 2002 reflects Congress' intent to leave undisturbed mission areas assigned to the DoD.⁷ Subsequent to the transfer of NCS management support to DHS, President Bush issued Homeland Security Presidential Directives (HSPDs) 5,⁸ 7⁹ and 8,¹⁰ which also recognize

³ See The Homeland Security Act of 2002, Public Law 107-296, November 25, 2002, § 201(g)(2).

⁴ U.S. Department of State, Central Intelligence Agency, U.S. Department of the Treasury, Federal Emergency Management Agency, U.S. Department of Defense, The Joint Staff, U.S. Department of Justice, General Services Administration, U.S. Department of Interior, National Aeronautics and Space Administration, U.S. Department of Agriculture, Nuclear Regulatory Commission, U.S. Department of Commerce, National Security Agency, U.S. Department of Health and Human Services, National Telecommunications and Information Administration, U.S. Department of Transportation, United States Postal Service, U.S. Department of Energy, Federal Reserve Board, U.S. Department of Veteran Affairs, Federal Communications Commission and U.S. Department of Homeland Security.

⁵ Assignment of National Security and Emergency Preparedness Telecommunications Functions", April 3, 1984

⁶ Amendment of Executive Orders and Other Actions In Connection With the Transfer of Certain Functions to the Secretary of Homeland Security", February 28, 2003.

⁷ E.g., P.L. 107-296, § 876. MILITARY ACTIVITIES provides in part: "Nothing in this Act shall ... limit the existing authority of the Department of Defense or the Armed Forces to engage in warfighting, the military defense of the United States, or other military activities."

⁸ See HSPD 5 <http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html> February 28, 2003 Subject: Management of Domestic Incidents paragraph (9), which states in part: "Nothing in this directive impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures. The Secretary of Defense shall provide military support to civil authorities for domestic incidents as directed by the President or when consistent with military readiness and appropriate under the circumstances and the law. The Secretary of Defense shall retain command of military forces providing civil support...."

continuing DoD responsibilities for such functions as military command and control, incident response and crisis communications.

The NCS is responsible for “the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution.”¹¹ In order to execute its assigned responsibilities in times of national emergency, domestic attack and crisis, robust, redundant, reliable communications will be essential if the DoD is to “... provide for the common defence...”¹² As the single largest user of national security emergency preparedness (NS/EP) priority services that are a crucial component of the NCS, the DoD strongly supports the comments filed on behalf of the Department of Homeland Security raising NCS equities for all NS/EP communications users, whether they are in the Federal, State, Local or Private Sector.¹³

⁹ See HSPD 7 <http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html> December 17, 2003 Subject: Critical Infrastructure Identification, Prioritization, and Protection paragraph (20), which states in part: “...Nothing in this directive shall limit the authority of the Secretary of Defense with regard to the command and control, training, planning, equipment, exercises, or employment of Department of Defense forces, or the allocation of Department of Defense resources.

¹⁰ See HSPD 8 <http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html> December 17, 2003 Subject: National Preparedness paragraph (20), which states in part: “...Nothing in this directive shall limit the authority of the Secretary of Defense with regard to the command and control, training, planning, equipment, exercises, or employment of Department of Defense forces, or the allocation of Department of Defense resources.

¹¹ EO 12472 directs that the NCS shall seek to ensure that a national telecommunications infrastructure is developed which: (1) Is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies and other entities, including telecommunications in support of national security leadership and continuity of government; (2) Is capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources; (3) Incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain, to the maximum extent practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency; and (4) Is consistent, to the maximum extent practicable, with other national telecommunications policies.

¹² Preamble to the Constitution of the United States, 1787.

¹³ IP-Enabled Services, WC Docket No. 04-36, Notice of Proposed Rulemaking, FCC 04-28 (Mar. 10, 2004) (IP Enabled Services), Pleading Cycle established in Public Notice DA-04-888 (WC Docket No. 04-36) of March 29, 2004 at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-04-888A1.pdf.

Impact of Emerging IP-Enabled Services on NS/EP Communications Priority Services

The DoD recognizes that the public switched telephone network (PSTN) is rapidly evolving to a primarily packet-switched Internet protocol (IP) technology-based infrastructure and it is critical that today's NS/EP services evolve accordingly. The Department believes that in the evolving IP-enabled environment both legacy voice telecommunications services and newly introduced information services must be utilized to meet NS/EP telecommunications requirements.¹⁴ These NS/EP services may require government regulatory consideration to ensure the NS/EP users receive the priority treatment they need to fulfill their missions during national emergencies. NS/EP considerations provide a compelling rationale for applying a certain amount of regulation to IP-enabled services.

In the Commission's recent "Decision on Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges" (FCC No. 04-97, WC Docket No. 02-361, adopted April 14, 2004, released April 21, 2004), AT&T's assertions that Internet protocol (IP) telephony services should be exempt from the access charges applicable to circuit-switched interexchange calls¹⁵ was deemed to be in error, based on interpretation of existing regulations. In that Order, the Commission clearly left open its options to determine in this pending rulemaking how it would regulate (or not regulate) such services in the future.

Users of NS/EP priority services expect ongoing changes in technology (such as voice over internet protocol [VoIP] and other packet-switched methodologies) to increasingly be

¹⁴ Report of the White House Convergence Task Force, December 29, 2000.

¹⁵ The "Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges" (filed Oct. 18, 2002) (AT&T Petition) led to the Commission's Order, FCC No. 04-97, WC Docket No. 02-361, adopted April 14, 2004, released April 21, 2004. AT&T had sought a declaratory ruling as to the applicability of interstate access charges to digital telephony services, and it asserted that such a ruling would provide guidance to states that mirror federal rules in assessing intrastate access charges.

adopted by commercial carriers and other major providers of services. Regardless of the means employed (circuit-switched or packet-switched), some structure is required in order to insure processes are in place when crisis communication actions are needed. Presently, given existing court opinions and this pending rulemaking, it is not clear to what extent the Commission will be able to either interpret or modify its existing regulations on priority services to allow for NS/EP IP-enabled priority services requirements which are likely to evolve as technologies converge.

The DoD asserts the public interest would be served by the Commission ensuring that priority treatment is provided for packet-switched NS/EP voice and data in a crisis, now and in the future. Any regulation of IP-based networks and IP-enabled services must preserve existing NS/EP telecommunications capabilities and allow for enhanced or evolving services as well. The current NS/EP services provided by the NCS are limited to voice telephony. In an IP-enabled communications environment, these services will need to be expanded to meet evolving NS/EP requirements beyond just voice. In times of emergency or network congestion, NS/EP priority treatment may be required for certain communications such as electronic mail, instant messaging, video feeds, or video conferencing sessions. The Commission's rulemaking process must address these concerns.

The DoD reminds the Commission that mixed applications of packet-switched technology (left largely unregulated) have still been deemed to be subject to the Commission's jurisdiction; for example, the Commission recently determined that the voice over internet protocol (VoIP) service provided by pulver.com's Free World Dialup is an unregulated information service that is subject to the Commission's jurisdiction.¹⁶ In the pending

¹⁶ Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service, WC Docket No. 03-45, Memorandum Opinion and Order, FCC 04-27 (Feb. 19, 2004).

rulemaking,¹⁷ the Commission has stated: “To the extent the market for IP-enabled services is not characterized by such monopoly conditions, we seek comment on whether there is a compelling rationale for applying traditional economic regulation to providers of IP-enabled services.” While DoD is not arguing for economic regulation, NS/EP considerations provide a compelling rationale for applying a certain amount of regulation to IP-enabled services. The purpose of such regulation would be to ensure the prioritized availability of certain communication services in times of emergency or national crisis.

DoD understands the NCS intends to take advantage of the technology developed by the industry to achieve its objectives of assured NS/EP communications during crises. The NCS also plans to continue to work with the industry through voluntary and contractual arrangements, subject to Congressional budget constraints, to support NS/EP services and features. If these voluntary and contractual arrangements are insufficient to achieve assured NS/EP IP-enabled communications services, the DoD would request the FCC consider imposing regulatory constraints on all providers of IP-enabled services (e.g., LECs, IXC, MSOs, ISPs, etc.).

PART II

STATEMENT OF INTEREST AND POSITION: SELECTED NATIONAL SECURITY-RELATED ROLES OF THE ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION, ASD/NII

Within the DoD, the Assistant Secretary of Defense for Networks and Information Integration, ASD(NII), is the Department’s Chief Information Officer (CIO),¹⁸ responsible for

¹⁷ IP-Enabled Services, WC Docket No. 04-36, Notice of Proposed Rulemaking, FCC 04-28 (Mar. 10, 2004) (IP Enabled Services), paragraph 5.

¹⁸ See 44 U.S.C., Chapter 35--Coordination of Federal Information Policy, Subchapter I--Federal Information Policy at http://www.access.gpo.gov/uscode/title44/chapter35_subchapteri.html , Subchapter II--Information Security at http://www.access.gpo.gov/uscode/title44/chapter35_subchapterii.html ; plus 40 U.S.C. Subtitle III --Information Technology Management Chapter 113--Responsibility For Acquisitions Of Information Technology, Subchapter II--Executive Agencies, Section 11315. Agency Chief Information Officer, as well as Chapter 111, Section 11103—Applicability to National Security Systems and 10 U.S.C. 2223, Information Technology: additional responsibilities

various information resource management functions. The ASD/NII also serves as the Chairman of what was originally called the National Security Telecommunications and Information Systems Security Committee (NSTISSC),¹⁹ but was renamed the Committee on National Security Systems (CNSS) by Executive Order (E.O.) 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001, as amended.²⁰ Changes to E.O. 13231 did not affect relevant DoD responsibilities assigned under prior Presidential Orders and Directives. The Secretary of Defense and the Director of Central Intelligence are responsible for developing and overseeing the implementation of government-wide policies, principles, standards, and guidelines for the security of systems with national security information.

This portion of the DoD's initial filing lists a few examples²¹ of the Department's ongoing activities that could be adversely impacted if the Commission fails to exercise some oversight over transmissions using internet protocol(s), related applications and packet-switched technology. Currently circuit-switched networks have the necessary technology in place to allow authorized elements of the DoD to access transmissions on the Department's networks, given appropriate legal authority. Ensuring appropriate technical means are implemented to permit similar access to DoD transmissions taking place in the IP-enabled services arena, would support the national defense in the U.S. A final section in this part suggests the Commission consider

of Chief Information Officers.

¹⁹ National Security Directive No. 42, entitled, "National Policy for the Security of National Security Telecommunications and Information Systems," dated July 5, 1990, superseded NSDD 145, dated September 17, 1984. It reaffirms the Secretary of Defense as the Executive Agent for National Security Telecommunications and Information Systems Security. The Directive established the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as an operating-level interagency group. For more details, see NSTISSD 900 - Governing Procedures of the National Security Telecommunications and Information Systems Security Committee (NSTISSC), dated April 2000, at http://www.nstissc.gov/Assets/pdf/nstissd_900.pdf.

²⁰ Per E.O. 13286, Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security, February 28, 2003.

²¹ Functions mentioned in these comments are intended to be illustrative, not exclusive; other equities and requirements may be identified by the DoD in the future.

some mechanism for providing a form of notice to components of the Executive Branch when non-domestic individuals or firms, or other foreign interests, purchase substantial interests in U.S. firms providing IP-enabled services/packet-switched transmission of data. To summarize the following sections in this filing, the DoD asserts that for both traditional telephone services, and IP-enabled services, similar technical access for lawful monitoring functions, and some form of administrative notice prior to significant foreign transactions being finalized, would be in the public interest.

A. Communications Security Monitoring Requirements

DoD needs to be able to monitor open/unsecured conversations and transmissions by our employees on our own systems (whether on circuit-switched or packet-switched equipment or networks) to ensure no classified information is improperly disclosed through unsecured transmissions. This crucial security assessment activity has been authorized for many years,²² and as technologies converge, DoD will need to ensure similar functions can continue with respect to evolving technology, regardless of the transmission mode employed by DoD people at work world-wide.

B. Ensuring Appropriate Use, and Combating Misuse, of DoD Systems

In addition to assessing how best to permit continued monitoring of Defense systems and networks for communications security purposes (covering both traditional and evolving technology transmissions), the Commission should also consider how failing to provide for monitoring mechanisms with respect to evolving transmission technologies could complicate legitimate oversight and investigative responsibilities assigned to the DoD.

²² See DoD Directive (DoDD) 4640.6 Communications Security Telephone Monitoring and Recording, June 26, 1981, USD(P) http://www.dtic.mil/whs/directives/corres/pdf/d46406_062681/d46406p.pdf as well as NTISS

1. Applying 47 U.S.C. § 222 to IP-Enabled Services and Service Provider Requirements

The Commission's extensive discussion in the current rulemaking raises a number of issues for possible comment.²³ In paragraph 37, the Commission invites "... commenters to address any other characteristic that should guide our decisions in this proceeding..." and also asks "Should the Commission differentiate between services offered on a 'common carriage' and 'private carriage' basis?". Later in its NPRM, the Commission raises the issue of how sensitive 'customer' (or user) data should be treated in the IP-enabled services arena, specifically raising customer proprietary network information (CPNI)²⁴ and whether the CPNI requirements (applicable to telecommunications carriers) should apply to any provider of VoIP or other IP-enabled services. It is DoD's position that the provisions of 47 USC Section 222 reflect a careful balance of the need to protect customer privacy while allowing telecommunications carriers the ability to protect the integrity of their networks. It is appropriate that IP-enabled service providers that are effectively offering their services as common carriage should be subject to these same rules. However, DOD does not see the need for additional privacy protections beyond those provided in Section 222. Furthermore, the customer privacy concerns with respect to private carriage are appropriately left to the parties to negotiate. This position reflects DOD's experiences both as a customer and as a service provider.

As a service provider, DoD has ongoing requirements for access to addressing data and transmitted content (previously carried over the Public Switched Telephone Network, PSTN) which is increasing carried over packet-switched networks and systems via Internet protocol (IP)

Directive (NTISSD) 600, (U) Communications Security (COMSEC) Monitoring, 10 April 1990 (FOUO.)

²³ E.g., paragraph 1 provides in part: "In this Notice of Proposed Rulemaking (Notice), we examine issues relating to services and applications making use of Internet Protocol (IP), including but not limited to voice over IP (VoIP) services... We seek comment on the impact that IP-enabled services, many of which are accessed over the Internet, have had and will continue to have on the United States' communications landscape....."

²⁴ See ¶ 71, and 47 U.S.C. § 222, Privacy of Customer Information.

applications and which transit DOD systems. Neither the means of transmission (whether circuit or packet-switched) nor the regulatory or semantic category of the services (telecommunications services or information services²⁵) alters DoD's need for access to information on its own systems. Building on the existing legislative and regulatory framework would avoid inadvertent exclusion of key policy and implemented practices necessary which DOD has found vital to protect Defense data and systems and which must also be true for commercial service providers. The Department functions as a major telecommunications and information technology 'Service Provider' in support of its assigned national security roles. Service Providers focus mainly on two primary functions: one is managerial, providing communications and data storage 'services' for 'users'; and the second is security-related, protecting the rights and property of the Service Provider. These two functions are recognized in U.S. statutes such as the Wiretap Statute,²⁶ and the Pen/Trap Statute.²⁷ Both contain specific exceptions, which allow Service Providers to intercept content and non-content (addressing information) communications on their networks in order to protect the rights or property of the provider. The Secretary of Defense has the responsibility to protect and defend DoD information, information systems, and information networks that are critical to the Department and the armed forces during day-to-day operations and in times of crisis.²⁸ From an information assurance (IA) perspective, in addition to statutory mandates from Congress, as implemented by memoranda from the Office of Management and Budget, internal DoD guidance requires that the Department's information systems "... shall be

²⁵ Paragraph 27 provides in part: "... the 1996 Act defined 'information service' to mean 'the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications network or the management of a telecommunications service.' the Commission has exercised its ancillary authority under Title I of the Act to apply requirements to information services..."

²⁶ 18 U.S.C. § 2511(2)(a)(i).

²⁷ 18 U.S.C. § 3121(b), Pen Registers and Trap and Trace Devices, commonly referred to as the Pen/Trap Statute.

²⁸ 10 U.S.C. § 2224, Defense Information Assurance Program, as implemented by various Departmental directives,

monitored based on the assigned mission assurance category and assessed risk in order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the IA of DoD operations or IT resources, including internal misuse..."²⁹ Shifting too fast and too far with respect to "customer privacy issues, separate from those raised in section 222 of the Act" as well as permitting unrestrained changes to commercial transmission technologies could make providing for the security and self-protection of DoD systems and networks problematic at best.

As video, voice and data proliferate on converging networks, the Department will still need to be able to manage its networks as a Service Provider to "... maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness."³⁰ Since the DoD purchases transmission services from a variety of commercial carriers and data service providers, the Commission can play a key role in encouraging (perhaps even enforcing) adherence to well-understood standards of privacy, service and security that would facilitate the Department's network information security and self-protection requirements.³¹ The Commission has asked for comments on whether it should consider additional customer privacy issues separate from those addressed in Section 222,³² as a sizable

regulations and instructions.

²⁹ See DoDD 8500.1, Information Assurance (IA), October 24, 2002, ASD(C3I) (Certified Current as of November 21, 2003) http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf, paragraph 4.20.

³⁰ Id. at paragraph 4.2.

³¹ For details see DoD I 8500.2 Information Assurance (IA) Implementation February 6, 2003 ASD(NII) http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf and CJCS Instruction 6211.02B Defense Information System Network (DISN): Policy, Responsibilities and Processes (31 July 2003) http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf.

³² See paragraph 77: "To the extent that we determine IP-enabled services are information services, we seek comment on whether there are any other policy priorities that we should consider. For example, to what extent, if any, do our policy priorities for IP-enabled services assume an underlying open network architecture? Will our

non-commercial organizational provider of IP-enabled services, DoD respectfully recommends that the current protections in Section 222 are sufficient and should be extended only to those IP-enabled service providers effectively engaged in common carriage.

2. DoD Inspectors General and Law Enforcement Requirements

In accordance with the Inspector General Act of 1978,³³ the DoD and Military Service Inspectors General have established responsibilities to investigate allegations of fraud, waste and abuse.³⁴ In some instances, DoD's own law enforcement components may need to apply technology to gain data needed to halt and/or punish wrongful actions involving DoD networks and systems.³⁵ In other cases, elements of the Department of Justice or the Department of Homeland Security may take a lead role in certain allegations of misconduct or crime involving DoD networks and systems. As a result, on its own behalf, and in support of the comments of the Department Justice and the Department of Homeland Security, DoD urges the Commission to give due consideration to law enforcement and public safety requirements in assessing how best to address IP-enabled services in this proceeding.

C. Notice of Foreign Transactions -- Carriers Who Seek to Provide International IP-Enabled Services Present Many of the Same Concerns as Traditional Applicants Seeking to Provide International Telecommunications Services.

National security issues of concern to the DoD can arise when a carrier seeks to provide

decisions in this proceeding affect the incentives of facilities-based IP service providers to provide network access to non-facilities based IP service providers? Will the incentives of facilities-based and non-facilities-based IP service providers differ? How should our policies differ with a closed or proprietary architecture? Similarly, are there customer privacy issues, separate from those raised in section 222 of the Act, that this Commission should consider?"

³³ Public Law 95-452, codified at Title 5, U.S.C., Appendix

³⁴ Within the DoD, implementing directives include: DoDD 5106.1 Inspector General of the Department of Defense; DoDD 5200.26 Defense Investigative Program; and DoD Instruction (DoDI) 5505.2, Criminal Investigations of Fraud Offenses. The Joint Ethics Regulation (JER, DoD 5500.7-R) paragraph 1-413 states: "The Inspector General of each DoD Component shall: a. Investigate ethics matters arising in the DoD Component, and refer any such matters that involve suspected criminal violations to the appropriate criminal investigative office of the DoD Component ..."

³⁵ See also DoDD 5505.9 Interception of Wire, Electronic, and Oral Communications for Law Enforcement, April

international communications service(s.) Such concerns arise regardless of whether a carrier provides traditional circuit-switched telecommunications service(s), or packet-switched/IP-enabled service(s). The means DoD needs to receive prior notice with respect to telecommunications services (in order to be able to address national security and national defense concerns) are provided for in existing law.³⁶ As recently as this month the DoD again stressed the vital importance of Section 214 review requirements when it filed comments opposing exceptions to the Commission's authorization requirements involving foreign entities. See Comments of the Department of Defense, *In the matter of Amendment of Parts 1 and 63 of the Commission's Rules*, IB Docket No. 04-47. The Department asserts the potential ability (or abilities) to damage law enforcement and national security interests are created by a provider's control over access to the communications, not by the particular technical means or protocol(s) a provider may employ to provide the communications capability. As a result, the Commission may determine (as DoD suggests) that a pre-transaction notice requirement would serve an important function; allowing appropriate Executive Branch agencies (those with responsibility for such areas as national security, infrastructure protection, law enforcement, foreign policy and trade policy) to consider whether a particular application may affect any of these interests before service begins.

One of DoD's concerns is that nearly all network applications (to include voice communications) are becoming (at least in part) Internet protocol (IP) services. For example, there are DoD organizations that have mixed Public Switched Telephone Network and VoIP

20, 1995, IG, DoD http://www.dtic.mil/whs/directives/corres/pdf/d55059_042095/d55059p.pdf.

³⁶ See 47 U.S.C. § 214(b) Notification of Secretary of Defense, Secretary of State, and State Governor, which states: Upon receipt of an application for any such certificate, the Commission shall cause notice thereof to be given to, and shall cause a copy of such application to be filed with, the Secretary of Defense, the Secretary of State (with respect to such applications involving service to foreign points), and the Governor of each State in which such line is proposed to be constructed, extended, acquired, or operated, or in which such discontinuance, reduction, or

communications systems. Depending on the outcome of this and other pending Commission rulemaking proceedings, in the future such transactions might potentially fall outside both the Telecommunications Act³⁷ and the Communications Assistance to Law Enforcement Act,³⁸ negating useful purposes served by related FCC regulations. If the Commission's published regulations do not keep pace with technology, the Department's ability to ensure compliance with other important Defense directives and policies could be adversely affected. The DoD supports Justice's position that IP Enabled Services should not be determined to fall outside relevant laws enacted to serve the public interest, nor should these IP-enabled services be ruled to fall outside the crucial structure and oversight the Commission is uniquely qualified to provide.

Conclusion

The Department of Defense asserts the public interest would be served by considering national security interests and requirements for both the telecommunications and the information technology infrastructures (as described above) in formulating any IP-enabled services regulations the Commission may deem it appropriate to issue, both with respect to issues raised in these comments relating to the Department's role as a member of the NCS, and with respect to possible impact on DoD's own ongoing national security-related activities.

impairment of service is proposed, with the right to those notified to be heard; and the Commission may require such published notice as it shall determine.

³⁷ The Telecommunications Act of 1996, Pub.L.104 –104, amended The Telecommunications Act of 1934; these Acts are codified at 47 U.S.C. §151 et seq.

³⁸ Public Law 103-414, October 1994.

Respectfully submitted,



CARL WAYNE SMITH
General Counsel
Defense Information Systems Agency
701 S. Courthouse Road
Arlington, VA 22204
(703) 607-6759



HILLARY J. MORGAN
Trial Attorney, Regulatory and International Law
Defense Information Systems Agency
701 S. Courthouse Road
Arlington, VA 22204
(703) 607-6092



KEITH R. ALICH, LT COL, USAF
Attorney-Advisor
Defense Information Systems Agency
701 S. Courthouse Road
Arlington, VA 22204
(703) 607-6096

June 10, 2004

Date Signed